

Berufsbegleitender Masterstudiengang
Informationsrecht (LL.M.)



PD Dr. Irimi Vassilaki

Computer- und Internet-Strafrecht

Impressum

Autorin: PD Dr. Iriini Vassilaki

Herausgeber: Universität Oldenburg, Center für lebenslanges Lernen C3L

Auflage: 9. Auflage, Erstausgabe 2007

Copyright: Vervielfachung oder Nachdruck auch auszugsweise zum Zwecke einer Veröffentlichung durch Dritte nur mit Zustimmung der Herausgeber, 2007 - 2015

Oldenburg, August 2015

INHALTSVERZEICHNIS

I.	EINFÜHRUNG – KRIMINOLOGISCHE GRUNDLAGEN	6
1	Wirtschaftsdelikte	11
2	Delikte gegen den demokratischen Rechtsstaat	24
3	Delikte gegen die Persönlichkeit i.w.S.	27
4	Delikte gegen die Jugend i.w.S.	31
II.	ANWENDUNG DES DEUTSCHEN STRAFRECHTS... 35	
1	Grundlagen des deutschen internationalen Strafrechts.....	35
2	Besonderheiten des IT-Strafrechts	36
2.1	Feststellung des Tatorts.....	37
2.2	Restriktive Auslegung von § 9 Abs. 1 StGB.....	37
2.3	Restriktive Anwendbarkeit von § 9 StGB.....	38
2.4	Anlehnung an die Anknüpfungspunkte des § 7 StGB	39
2.5	Eigenständige Auslegung des Merkmals „zum Tatbestand gehörender Erfolg“ des § 9 Abs. 1 Alt. 3 StGB.....	40
III.	VORSCHRIFTEN DES STRAFGESETZBUCHS	44
1	Gefährdung des demokratischen Rechtsstaats und der öffentlichen Ordnung.....	44
1.1	Schriftenbegriff des § 11 Abs. 3 StGB.....	44
1.2	Verbreitung von Propaganda verfassungswidriger Organisationen.....	46
1.3	Kennzeichen verfassungswidriger Organisationen (§ 86a StGB).....	51
1.4	Öffentliche Aufforderung zu Straftaten (§ 111 StGB).....	54
1.5	Volksverhetzung (§ 130 StGB)	56
1.6	Anleitung zu Straftaten (§ 130a StGB)	61
1.7	Gewaltdarstellung (§ 131 StGB)	62
2	Verbreitung pornographischer Schriften (§ 184 bis 184c StGB).....	65
2.1	Objektiver Tatbestand	65
2.2	Subjektiver Tatbestand	71
2.3	Konkurrenzen.....	72
2.4	§ 184c StGB.....	72
3	Ausspähen von Daten (§ 202a StGB)	74
3.1	Objektiver Tatbestand	74
3.2	Subjektiver Tatbestand	78
3.3	Strafantrag	78

4	Abfangen von Daten (§ 202b StGB)	78
4.1	Objektiver Tatbestand	79
4.2	Subjektiver Tatbestand	80
4.3	Rechtswidrigkeit.....	80
4.4	Strafantrag	80
4.5	Subsidiaritätsklausel	80
5	Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)	81
5.1	Objektiver Tatbestand	81
5.2	Subjektiver Tatbestand	84
5.3	Strafverfolgung.....	84
6	Schutz von Berufsgeheimnissen (§§ 203, 204 StGB) ...	85
6.1	Tatobjekt und Tathandlung (§ 203 StGB)	85
6.2	Tatobjekt und Tathandlung (§ 203 Abs. 2 StGB)	87
6.3	Tatobjekt und Tathandlung (§ 204 StGB)	87
6.4	Einwilligung	87
6.5	Strafantrag	88
7	Computerbetrug (§ 263a StGB)	88
7.1	Objektiver Tatbestand	88
7.2	Subjektiver Tatbestand	94
7.3	Vorbereitungshandlungen.....	94
7.4	Rechtswidrigkeit, Konkurrenzen, Strafantrag	95
8	Datenveränderung und Computersabotage (§ 303a und § 303b StGB)	96
8.1	Datenveränderung (§ 303a StGB)	96
8.2	Computersabotage (§ 303b StGB).....	100
IV.	NEBENSTRAFRECHTLICHE VORSCHRIFTEN	106
1	Urheberstrafrecht (§§ 106 ff. UrhG)	106
1.1	Rechtsgut	106
1.2	Strafbares Verhalten	106
1.3	Ordnungswidrigkeit nach UrhG	109
1.4	Das Merkmal „Einwilligung“ des § 106 UrhG	109
1.5	Urheberrechtlicher Schutz von Datenbanken	113
1.6	Akteneinsicht bei Urheberrechtsverletzungen	113
2	Wettbewerbsstrafrecht (§§ 17, 18 UWG)	115
2.1	Tatobjekt	115
2.2	Geheimnisverrat.....	115
2.3	Betriebsspionage bzw. unbefugtes Ausspähen von Geheimnissen	116
2.4	Geheimnisverwertung	117
2.5	Vorlagenfreibeuterei.....	118

3	Datenschutzstrafrecht	119
3.1	Ordnungswidrigkeiten des BDSG (§ 43 BDSG)	119
3.2	Strafvorschriften (§ 44 BDSG)	120
4	Jugendschutzstrafrecht	
	(§§ 27, 28 Jugendschutzgesetz)	123
4.1	Strafvorschriften des Jugendschutzgesetzes	
	(§ 27 Jugendschutzgesetz)	124
4.2	Ordnungswidrigkeiten des Jugendschutzgesetzes	125
4.3	Strafvorschrift des JMStV	126
4.4	Ordnungswidrigkeiten des JMStV	128
	LITERATUR.....	129
	MUSTERLÖSUNGEN.....	142

I. EINFÜHRUNG – KRIMINOLOGISCHE GRUNDLAGEN

Es gibt keine umfassenden wissenschaftlichen Untersuchungen, die belegen können, wie oft die neuen Medien für die Begehung von Straftaten missbraucht werden, welche Straftatbestände und wie häufig diese erfüllt werden oder wie hoch die Schäden aus dieser Kriminalitätsform sind.¹ Mehrfach fällt in diesem Zusammenhang das Stichwort „Kinderpornographie“ oder „Volksverhetzung“. Die Verbindung des Missbrauchs von neuen Telekommunikationsmedien mit der Verbreitung von pornographischen oder staatsgefährdenden Inhalten würde dieser Kriminalitätsform nicht gerecht, denn ein oberflächliches Durchblättern der strafrechtlichen Entscheidungen, die sich mit dieser Frage beschäftigen, weist schon darauf hin, dass die „multimediale Kriminalität“² oder die „Internet- oder „Post-Computerkriminalität“³ viele Erscheinungsformen hat. Es trifft wohl zu, dass keine sicheren Angaben hinsichtlich der Erscheinungsformen der multimedialen Kriminalität gemacht werden können, weil einschlägige kriminologische Analysen fehlen.⁴

Das Bundeskriminalamt (BKA) hat für 2010 mehr Straftaten im Bereich der Computerkriminalität festgestellt. Besonders beim Ausspähen und Abfangen von Daten ist ein Anstieg der Straftaten aufgefallen. Bei den Straftaten, bei denen das Internet als Tatmittel eingesetzt wird, handelt es sich der polizeilichen Kriminalstatistik zufolge hauptsächlich um Waren- und Warenkreditbetrug. Der Betrug mit Zahlungskarten, bei denen die Täter die Daten nicht rechtmäßig erworben haben, hat um 11,9 Prozentpunkte zugenommen. Insgesamt handelt es sich deutschlandweit im Jahr 2010 um 19.100 Fälle.

In 15 Bundesländern (eines wurde wegen 2009 fehlender Daten nicht mitgerechnet) wurden 2010 insgesamt 223.642 Straftaten erfasst, die über das Internet begangen wurden. Gegenüber 2009 ist dieser Wert um 8,1 Prozentpunkte angestiegen, in absoluten Zahlen ist das bislang der höchste Wert. Zu 81,6 Prozent handelt es sich dabei um Betrugsdelikte. Auch die Zahl der Fälle von Computerbetrug ist gestiegen, um 8,0 Prozentpunkte. Einen auffälligen Anstieg verzeichnen die Statistiker der Polizei beim Ausspähen und Abfangen von Daten. Hier hat sich die Zahl der Delikte von 3,3 Prozent auf 4,2 Prozent erhöht. Die Computerkriminalität insgesamt stieg 2010 um 12,6 Prozentpunkte auf 84.377 Fälle. Die

¹ S. auch Gercke, ZUM 2010, S. 638.

² Zu diesem Begriff Vassilaki, CR 1997, S. 297; dazu auch Barton, Multimedia Strafrecht, 1999, S. 34; Bremer, Strafbare Internet-Inhalte in internationaler Hinsicht, 2001, S. 61; Dornsreif/Schumann/Klein, DuD 2002, S. 226.

³ Vgl. dazu Vassilaki, MMR 2006, S. 212.

⁴ S. dazu Shimada, CR 2009, S. 689., der für die Bestrafung der Internetkriminalität die Notwendigkeit der „Vorfelddkriminalisierung“ heranzieht.

Behörden berichten, dass Betrug, Kinderpornographie und sexueller Missbrauch immer stärker in Zusammenhang mit neuen Informationstechnologien stünden.

Über alle Straftaten gesehen ist die Zahl der Fälle seit 1993 um 12,1 Prozent zurückgegangen. Die Aufklärungsquote erhöhte sich in diesem Zeitraum von 43,8 auf 56 Prozent. Im Bereich der Computerkriminalität dagegen konnte die Polizei weniger Delikte aufklären: Bei der Computersabotage sank die Aufklärungsquote um 4,8 Prozentpunkte, beim Betrug mit Internet- und Kommunikationsmitteln um 2,2 Prozentpunkte.⁵

Im Jahr 2011 ist das Bild gemischt. Nachdem 2010 Großverfahren im Zusammenhang mit Online-Auktionsplattformen abgeschlossen worden waren, ging der Warenbetrug im Internet 2011 deutlich zurück. Ohne Berücksichtigung des Warenbetrugs wäre die Internetkriminalität um fünf Prozent auf 15.425 Fälle gestiegen. Die digitale Schutzgelderpressung explodierte von zwei auf 2.899 Fälle. Besitz und Verschaffen von Kinderpornografie im Internet ist um ein Sechstel auf 327 Straftaten angewachsen.⁶

Die Bedrohung durch Cyberkriminalität in Deutschland nimmt laut einem Lagebericht des Bundeskriminalamts (www.bka.de) trotz stagnierender Fallzahlen weiter zu. Im Jahr 2011 hat es rund 60.000 Fälle von Internet-Kriminalität gegeben. Der verursachte Schaden ist um 16 Prozent auf schätzungsweise 71,2 Millionen Euro gestiegen. Die größte Straftatengruppe sei dabei der Computerbetrug gewesen: Mit Phishing-Mails und dem missbräuchlichen Einsatz von Kreditkartendaten ist ein Schaden von rund 50 Millionen Euro entstanden. Obwohl die kriminellen Aktivitäten zugenommen haben, ist die Dunkelziffer sehr hoch. Für die Verbreitung von Schadsoftware wurden vermehrt Botnetze genutzt. Das Phishing von Onlinebanking-Daten oder der missbräuchliche Einsatz von Kreditkartendaten machen mit 45 Prozent die mit Abstand größte Gruppe der Bedrohung aus. Ein zunehmend attraktives Ziel ist auch das Smartphone. Unternehmen sind von den Cyberattacken ebenso betroffen wie Privatnutzer. 40 Prozent der Unternehmen in Deutschland verzeichneten teils mehrmals Angriffe auf ihre IT-Systeme. Ein Drittel hat demnach bereits Erfahrungen mit dem Verlust von Daten gemacht.⁷

Im Jahr 2012 sind – laut der polizeilichen Kriminalstatistik 2012 – die in Deutschland im Internet erfassten Delikte sowie Straftaten mit Computerbezug im Vergleich zum Vorjahr um jeweils gut 3 Prozent angestiegen. Strafverfolger registrierten 229.408 Fälle von Kriminalität "unter Nutzung des Tatmittels Internet", wozu vor allem Betrugsdelikte zählen. 2011 waren es noch 222.267. Der Bereich Computerkriminalität umfasste 87.871 Vergehen statt 84.981 im Vorjahr. Straftaten, bei denen Täter moderne Informations- und Kommunikationstechnik (IuK) ausnutzen, indem sie etwa Daten ausspähen und abfangen, mit einer

⁵ PKS 2010, S. 5.

⁶ S. Polizeiliche Kriminalstatistik 2011.

⁷ BKA, Cybercrime, 2011, S. 6, 18.

Schadsoftware Informationen verändern oder Systeme beschädigen, sind 2012 im Vergleich zu 2011 um 7,5 Prozent auf 63.959 Fälle nach oben geschnellt. Besonders hoch ist die Zunahme um rund 130 Prozent bei Computersabotage etwa mit DDoS-Attacken und Datenveränderung von 4644 auf 10.857 Straftaten. Der Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten ging in diesem Sektor dagegen am stärksten um fast 38 Prozent auf 2952 Fälle zurück. Die Aufklärungsquote bei Cybercrime ist um 3,5 Prozentpunkte auf 26,5 Prozent und im Teilbereich Datenmanipulation und Sabotage massiv um 23,7 Prozentpunkte auf 17,5 Prozent zurückgegangen. Die Polizei geht bei Cyber- sowie Computerkriminalität insgesamt von einem "erheblichen Dunkelfeld" aus. In die Statistik gingen nur Taten ein, bei denen der Verdächtige in Deutschland am Computer sitzt. In vielen Fällen nutzten Kriminelle aber Server im Ausland und starteten ihre Angriffe auch von dort aus. Wie im Vorjahr nahm 2012 die Verbreitung pornographischer Schriften ab, und zwar um 11,6 Prozent auf 7709 Fälle. Ein Teilbereich davon ist der Besitz und die Verschaffung von Kinderpornographie, der ebenfalls weiter rückläufig ist: Er sank um 16,9 Prozent auf 3239 in die Statistik eingegangene Delikte. Die Aufklärungsquote ist hier um 1,2 Prozentpunkte angestiegen. Eine leichte Steigerung um 89 auf 2465 Fälle ist dagegen bei der Verbreitung von Inhalten rund um sexuellen Kindesmissbrauch festzustellen, während die Aufklärungsquote bei diesen Straftaten niedriger als im Vorjahr (67,7 statt 72,8 Prozent) war. Vergehen im Zusammenhang mit Urheberrechtsbestimmungen wiesen im Gegensatz zu 2011 wieder einen Anstieg um 5,6 Prozent auf 7417 Fälle auf. Insgesamt zählt die Statistik – wie in den beiden Jahren zuvor – weniger als 6 Millionen Vergehen. Gegenüber dem Vorjahr wuchs ihre Zahl geringfügig um 0,1 Prozent auf 5.997.040 Straftaten an. Die Aufklärungsquote lag fast unverändert bei 54,4 Prozent im Vergleich zu 54,7 Prozent 2011. Die Zahl der Tatverdächtigen reduzierte sich um 0,9 Prozent auf rund 2,10 Millionen Personen.⁸

Auch das Landeskriminalamt von Mecklenburg-Vorpommern erwartet eine weitere Zunahme von Straftaten mit Hilfe des Internets. Bereits für 2011 gab es in dem Bundesland einen Anstieg von 9,3 Prozent der Internetstraftaten auf 5304 Fälle. Schwerpunkt der Cyberkriminalität ist der Betrug beim Kauf und Verkauf von Waren. Aber auch Angriffe auf private Computer oder Behördenrechner mit Schadsoftware sowie das Ausspähen sensibler Daten und Sabotage nahmen zu. Selbst bei Polizeibehörden und dem Landeskriminalamt hätte es schon Hackerattaken gegeben.⁹

Laut einer Studie von Hewlett-Packard verursachen Datendiebstahl, Computerviren und Web-Attacken in einem deutschen Großunternehmen jährlich einen Schaden von durchschnittlich 4,8 Millionen Euro. Deutschland liegt in der Statistik damit zwischen den USA (6,9 Millionen Euro) und Japan (3,9 Millionen Euro). Pro Woche gibt es in den für die Studie untersuchten Unternehmen und Behörden 1,1 erfolgreiche Angriffe – verglichen mit 1,8 in den USA. Allein 40

⁸ Polizeiliche Kriminalstatistik 2012, S. 5.

⁹ www.heise.de/-1775338.

Prozent des geschätzten Schadens entfallen auf Datenverluste – oft verursacht durch "Taten krimineller Insider". Weitere 28 Prozent fallen als Umsatzeinbußen an, etwa wenn nach einer Denial-of-Service-Attacke die Shopping-Webseite lahmgelegt wird.¹⁰

International belegt eine neue Studie der Sicherheitsfirma Symantec, dass Privatpersonen weltweit rund 110 Milliarden US-Dollar (derzeit rund 88 Milliarden Euro) an finanziellen Schäden durch Cyberkriminalität erlitten haben. In dem erfassten Zeitraum von Juli 2011 bis Juli 2012 soll jedes Opfer im Schnitt 197 US-Dollar (rund 157 Euro) eingebüßt haben. Neuer Trend scheint der Missbrauch Sozialer Netzwerke und mobiler Geräte zu sein: 20% derer User wurden zum Opfer. Bei 15% wurde – laut Studie – der Social-Media-Account gekapert und 10% fielen auf falsche Links und Spam über soziale Netzwerke rein. Insgesamt glauben 75% der Befragten, dass die Cyberkriminellen immer stärker in sozialen Netzwerken aktiv werden.¹¹

Nach einer GfK-Studie ist fast jeder zweite Surfer (47,6 Prozent) schon einmal Opfer von Internetkriminalität geworden. Am häufigsten haben Betroffene mit Schadsoftware auf ihrem Rechner zu kämpfen (25,7 Prozent) oder fallen beim Online-Einkauf und bei Internet-Diensten Betrügern zum Opfer (16,8 Prozent). Viele Nutzer berichten über unbefugten Zugriff auf ihre persönlichen Daten sowie deren Missbrauch oder Diebstahl (10,9 Prozent). Auch vermeintlich kostenlose Dienstleistungen, für die später doch gezahlt werden muss, sind der Umfrage zufolge ein größeres Problem (10,8 Prozent). Für die Studie zum Safer Internet Day am 5. Februar waren insgesamt 1000 Internetnutzer repräsentativ befragt worden.¹²

Laut der Polizeilichen Kriminalstatistik (PKS) 2013 haben die Ermittlungsbehörden 64.426 Fälle und damit gegenüber dem Vorjahr einen Anstieg um 0,7 Prozent registriert. Im Teilbereich der Computersabotage und Datenveränderung schnellten die erfassten Fälle um 17,6 Prozent auf 12.766 nach oben. Diese Zunahme wird vor allem durch häufigere Angriffe durch Schadsoftware wie Trojaner erklärt. Zugleich sank die Aufklärungsquote in diesem Sektor von 17,5 auf 9,2 Prozent. Der erfasste Computerbetrug ist allerdings um 6,3 Prozent auf 23.242 Fälle zurückgegangen, die Aufklärungsquote hier sogar leicht auf 31,1 Prozent gestiegen. Ein Minus von 7,5 Prozent bei 2730 registrierten Taten weist die PKS beim Erschleichen von Zugangsberechtigungen zu Kommunikationsdiensten aus bei einer deutlich auf 42,6 Prozent nach oben gekletterten Quote der Ermittlungserfolge. Auch beim Ausspähen und Abfangen von Daten hat die Polizei weniger Straftaten erfasst: 15.909 im Vergleich zu 16.794 im Jahr zuvor. Die Aufklärungsquote liegt hier mit 18,3 Prozent etwas höher. Eine um 14,5 Prozent zunehmende Tendenz ist dagegen bei der Fälschung beweiserheblicher Informa-

¹⁰ 3rd Annual Cost of Cyber Crime Study, 2012.

¹¹ S. 2012 Cybercrime Report.

¹² <http://www.e-commerce-blog.de/2013/02/08/internetkriminalitat-eine-prasente-gefahr/8670/>.

tionen und der Täuschung im Rechtsverkehr bei der Datenverarbeitung mit 9779 Fällen festzustellen. Der übergeordnete Bereich der gesamten Computerkriminalität ist um 1 Prozent auf 88.722 erfasste Delikte angestiegen. Die Aufklärungsquote ist dabei leicht um 1,1 auf 28,8 Prozent zurückgegangen. Insgesamt wurden zudem 257.486 Fälle erfasst, die mithilfe des "Tatmittels Internet" begangen wurden, was einem Plus von 12,2 Prozent gleichkommt. Überwiegend handelte es sich dabei um Betrugsdelikte wie eine Online-Bestellung von Waren, für die nach Lieferung nicht gezahlt wird. Die 6597 Fälle pornografischer Schriften, die über das Internet verbreitet worden sind, machen 31,1 Prozent mehr als 2012 aus. Dieser Tatbereich macht 2,6 Prozent aller online begangenen Delikte aus. Die Aufklärungsquote ist in diesem Sektor um 3,8 Punkte angestiegen, rangiert nun bei 84,8 Prozent. Ein Teilbereich ist der Besitz und die Verschaffung von Kinderpornografie mit ebenfalls ansteigender Tendenz: plus 27,9 Prozent auf 4144 Fälle. Die seit dem Jahr 2009 zunehmende Zahl der Straftaten des sexuellen Kindesmissbrauchs ist im aktuellen Berichtsjahr erstmals wieder um 1,5 Prozent leicht rückläufig auf 12.437 Vorgänge. Generell hat die Polizei wie bereits in den beiden Vorjahren auch 2013 weniger als sechs Millionen Delikte registriert, nämlich genau 5.961.662. Die Aufklärungsquote liegt mit einem Wert von 54,5 Prozent ganz leicht über dem Niveau von 2012. Die Zahl der Tatverdächtigen ist mit etwas über zwei Millionen gegenüber dem Vorjahr konstant geblieben.¹³

Die Anzahl der auf Cybercrime entfallenden Straftaten ist laut PKS 2014 für das Jahr 2014 gegenüber den Vorjahren im Bundesdurchschnitt deutlich geringer, zugleich sind die Aufklärungsquoten gestiegen. Diese Zahlen sind mit der Tatsache verbunden, dass die PKS für das Jahr 2014 nur solche Straftaten erfasst hat, für die konkrete Anhaltspunkte vorliegen, dass die Tathandlung in Deutschland durchgeführt wurde. Auf dieser Grundlage wurden für 2014 49.925 Fälle registriert. Die Aufklärungsquote beträgt 29,3 Prozent und im Teilbereich „Datenveränderung und Computersabotage“ 17,7 Prozent (2013: 9,2 Prozent). Insgesamt wurden im Jahr 2014 73.900 Fälle von „Computerkriminalität“ registriert, darunter 11.887 Fälle von „Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen“ sowie 5.661 Fälle von „Datenveränderung und Computersabotage“.¹⁴

Nach einer Bitkom-Umfrage seien 55% der Befragten im Jahr 2013 Opfer von Cybercrime geworden. Hochgerechnet wären dies also 29 Millionen Bundesbürger, die unter Cybercrime-Attacken gelitten hätten. Bei 40% der Befragten sei der Computer mit Schadprogrammen infiziert worden. 47% der Befragten verschicken vertrauliche Texte nicht mehr per Internet-Mail, 16% der Befragten verschlüsseln die Emails. Im Vorjahr waren dies nur 6 Prozent. Schwächer fiel der

¹³ Siehe Polizeiliche Kriminalstatistik 2013, S. 11, 81, Cybercrime Bundeslagebild 2013.

¹⁴ PKS 2014, S. 6, 12, 13.

Anstieg bei der Nutzung von Anonymisierungsdiensten wie Tor aus; er stieg von 11 auf 16 Prozent.¹⁵

Mithin ist das Gefährdungs- und Schadenspotenzial des Phänomens Cybercrime unverändert hoch.¹⁶

Aus den durch die Presse bekannt gewordenen als auch aus den von Strafgerichten judizierten Fällen lassen sich folgende Kategorien bilden, die den Missbrauch der neuen Telekommunikationsmedien betreffen:

- Wirtschaftsdelikte
- Delikte gegen den demokratischen Rechtsstaat
- Delikte gegen die Persönlichkeit i.w.S.
- Delikte gegen die Jugend i.w.S.

1 Wirtschaftsdelikte

Dass die neuen Informationstechnologien für den Abschluss und die Durchführung von Geschäften verwendet werden, ist eine Binsenwahrheit. Aus diesem Grund liegt es nahe, dass E-Commerce ein beliebtes Betätigungsfeld für Kriminelle darstellt. In diesem Zusammenhang erfasst diese Kategorie der multimedialen Kriminalität jede Tätigkeit, die die Erscheinungsformen des E-Commerce missbraucht, um finanzielle Vorteile für den Täter zu erlangen. Die Manipulationen, die im Zuge des Ablaufs etwa von Online-Auktionen durchgeführt werden, die strafbaren urheberrechtlichen Verletzungen bei der Online Übermittlung etwa von Software oder Musik oder die Verletzung von Geschäftsgeheimnissen während der Online-Nutzung einer Datenbank, stellen nur ein paar Beispiele dar, die den wirtschaftlichen Teil des Medienstrafrechts bilden.

Insbesondere fördert der unkörperliche Kontext des "Cyberraums" die Verletzung des geistigen Eigentums. Im Jahr 2010 wurden in Deutschland Programme im Wert von rund 1,6 Milliarden Euro raubkopiert. 27 Prozent aller verwendeten Programme sind illegal. In der EU stagniert der Anteil unlizenzierter Software bei 35 Prozent. Der Wert stieg allerdings von 8,3 auf umgerechnet 10,1 Milliarden Euro. Was das Volumen der Raubkopien angeht, liegen weltweit die USA (20 Prozent, 9,5 Milliarden US-Dollar), China (78 Prozent, 7,8 Milliarden US-Dollar) und Russland (65 Prozent, 2,8 Milliarden US-Dollar) an der Spitze.¹⁷ Nach der "Brennerstudie 2010" geht die Zahl der illegalen Musikdownloads zurück. Die Zahl der illegalen Musikdownloads sank von 316 Millionen in 2008 auf 258 Millionen in 2009. Der typische Filesharer ist männlich und 20-39 Jahre alt. Von den rund 4,5 Millionen Deutschen, die sich il-

¹⁵ Siehe dazu

http://www.bka.de/DE/Presse/Pressemitteilungen/Presse2014/140827__BundeslagebildCybercrime.html?_nnn=true

¹⁶ BKA, Cybercrime 2010, Bundeslagebild 2010, S. 14.

¹⁷ S. Eighth Annual BSA Global Piracy Study (2010).

legal mit Musik, Filmen, Games oder (Hör-)Büchern aus dem Internet versorgen, sind in der Altersgruppe der 20- bis 29-jährigen Männer mit 25 Prozent und bei den 30- bis 39-jährigen Männern mit 17 Prozent die meisten Filesharer zu finden. Dies zeigt, dass es sich bei Tauschbörsennutzern nicht überwiegend um Kinder und Jugendliche handelt. Nach den Zahlen nutzte unter den 10- bis 19-Jährigen nicht mal jeder zehnte Jugendliche (9 Prozent) die illegalen Angebote.¹⁸

Die AfD-Studie "Online-Filmpiraterie transparent gemacht" hebt hervor, dass 65% aller Filme als Raubkopien in den Tauschbörsen erscheinen. Davon taucht 1/3 schon vor dem Kinostart oder am Startwochenende im Internet auf, während 45% in den ersten beiden Wochen nach der Premiere im Internet verfügbar ist. Der Online-Anteil der Filmpiraterie in den Vereinigten Staaten und Großbritannien ist hoch. In Deutschland liegt er im Mittelfeld.¹⁹

Ende August 2014 hat ein Gericht im englischen Wolverhampton einen 25-Jährigen zu 33 Monaten Gefängnis verurteilt, der Filme illegal aufgezeichnet, im Netz verbreitet und verkauft hatte. Sein Mitangeklagter wurde zu 120 Sozialstunden verurteilt. Der Hauptangeklagte hat im Mai 2013 eine Kinovorstellung des US-Films "Fast and Furious 6" mit einem Camcorder abgefilmt und im Netz verbreitet. Nach Angaben der britischen Federation Against Copyright Theft (FACT) war das die erste illegale Kopie des Streifens im Netz und wurde rund 700.000 Mal heruntergeladen. FACT beziffert den dem Filmstudio und der britischen Branche entstandenen Schaden auf "mehrere Millionen Pfund". Laut FACT wirkte strafverschärfend, dass der Verurteilte den Streifen nicht nur gratis im Netz verbreitet hat, sondern Kopien auch von anderen Filmen wie "Iron Man 3" für 1,50 Pfund (1,90 Euro) über Facebook verkauft hat. Zudem soll Philip D. weitere Filme illegal verbreitet haben, auch nachdem er festgenommen und vernommen worden war.²⁰

Gleichwohl weist eine Umfrage des Instituts American Assembly der Columbia University im Rahmen der Studie „Copy Culture in the US and Germany“ darauf hin, dass US-amerikanische Erwachsene, die an Tauschbörsen teilnehmen, durchschnittlich eine größere Sammlung an digitalen Musiktiteln besitzen als jene, die kein File-sharing betreiben. Dieses Ergebnis klingt nicht überraschend. Die Tauschbörsenteilnehmer geben auch mehr Geld für Musikstücke aus als die Nicht-P2P-Nutzer.²¹

Der Bundesverband der Musikindustrie (BVMI) hat gemeldet, dass im Jahr 2012 die legalen Downloads um 22,4% gestiegen sind. Von den knapp 115 Millionen Downloads entfallen 97 Millionen auf einzelne Tracks (+22,9 Prozent), 16 Millionen und damit 55 Prozent aller Downloadumsätze auf komplette Alben (+20,6 Prozent) und 1,5 Millionen auf Single-Bundles (+12,8 Prozent).²²

¹⁸ Siehe die Ergebnisse der Brennerstudie 2010.

¹⁹ AfD-Studie, Online-Filmpiraterie transparent gemacht, 2005, S. 4 (5).

²⁰ Siehe dazu <http://www.fact-uk.org.uk/cammer-sentenced-to-33-months-imprisonment/>.

²¹ Copy Culture in the US and Germany, S. 47.

²² http://www.musikindustrie.de/presse_aktuell_einzel/back/82/news/mehr-als-100-millionen-legale-musikdownloads-in-2012/

Wie eine Studie, die die Firma McAfee in Auftrag gegeben hat, darlegt, werden die Informationstechnologien von organisierten Kriminellen angewendet, um Gewinne aus Straftaten, etwa durch Betrug, Erpressung und Kindesmissbrauch zu erzielen. Dafür werden professionelle Hacker oder Viren-Programmierer angeheuert, die auf Bestellung Eingriffe gegen Netzwerke vorbereiten und durchführen.²³ "Hacking" ist bereits seit den achtziger Jahren eine bekannte Form der Computerkriminalität. Die Attacken auf Informationssysteme haben in den letzten zehn Jahren einen anderen Charakter angenommen. Das Motiv der Täter ist nicht – wie in den 80er Jahren – nur in der Herausforderung zu suchen, technische Systeme zu knacken. Bei den meisten Angreifern handelt es sich nun um Hacker, die bezahlt werden, um die Sicherheitsmaßnahmen von Computernetzen zu überwinden, Daten zu manipulieren oder Netzwerke zu beschädigen. Angreifer dringen in großer Zahl in Netzwerken ein und verursachen absichtlich Schäden in Millionenhöhe. Bezeichnend für diese Entwicklung ist der sog. "Liquid FX-Fall". Im März 2004 haben 15 Polizeigruppen 132 Wohnungen von Mitgliedern des Hackerforums "Liquid FX" durchsucht. Die Ermittlungen, die zur Anklage von 126 Hackern führten, ergaben, dass es sich bei "Liquid FX" um eine grenzüberschreitende Organisation handelte, der 476 Mitglieder aus 33 Ländern angehörten. Sie betrieben 11.820 "Zombies"²⁴ in 83 Ländern, von denen 619 in Deutschland festgestellt worden waren. Sie wurden verwendet, um Raubkopien von Software, Musik und Filmdateien zu speichern.²⁵

Aus diesem Hackerprofil soll der „Hackeraktivist“ differenziert werden. Dieser ist ein Hacker, dessen Ausübung von Taten nicht-profitorientiert und ideologisch motiviert und zum Zwecke des Protests und der Propaganda aus ist. Außerdem der Hackeraktivismus wird überwiegend von Gruppierungen ausgeübt. der Hackeraktivist ist - einer BKA-Untersuchung zufolge - in 90% der Fälle männlichen Geschlechts und zwischen 18 und 30 Jahren alt.²⁶

Mit einem virusähnlichen Programm bemächtigten sich Hacker im Juni 2005 in den USA der Daten von über 40 Mio. Kreditkarteninhabern. Die Täter drangen in das Computersystem einer Firma ein, die Transaktionen zwischen Konsumenten, Handel und Kreditkartenfirmen abwickelt. Das Unternehmen VISA teilte mit, dass bei ca. 40.000 dieser Karten die Inhalte der Magnetstreifen entwendet wurden, so dass größte Betrugsgefahr bestand.²⁷

Schadsoftware wurde über Terminals in den Ladengeschäften der Firma „Neiman Marcus“ eingeschleust und vom 16. Juli bis 30. Oktober 2013 sammelte diese

²³ Siehe dazu Bericht von McAfee zum Thema virtuelle Kriminalität, Februar 2005, S. 6.; auch Vassilaki, MMR 9/2003, S. V.

²⁴ Zombies sind infizierte Computer, die sich unter der Kontrolle einer anderen Person als des rechtmäßigen Nutzers befinden.

²⁵ So der Bericht von McAfee zum Thema virtuelle Kriminalität, S. 8.

²⁶ BKA, Hackaktivisten., S. 70.

²⁷ Siehe den Bericht in <http://www.stern.de/wirtschaft/unternehmen/541977.html?nv=cb>.

Kartendaten. Die Software hätte dabei auf 1,1 Millionen Datensätze zugreifen können. Visa, MasterCard und Discover hätten bislang von 2400 Missbrauchsfällen berichtet, die mit dem Datendiebstahl in Verbindung stünden.²⁸

Im April 2013 haben durch den Einsatz einen sog. Carberp-Trojaner Kriminellen aus der Ukraine und Russland rund acht Milliarden russische Rubel und drei Millionen ukrainische Griwna erbeutet – umgerechnet etwa 200 Millionen Euro. Die betroffene Sberbank meldete, dass die Kriminellen Trojaner der Carberp-Familie anwendeten, weiterentwickelten und -verkauften. Anführer der Bande war ein 28-jähriger Russe aus der ukrainischen Schwarzmeerstadt Odessa. Den Hackern drohen jeweils bis zu sechs Jahre Haft. Erst vor einigen Wochen wurde eine Gruppe von Kriminellen in Russland verhaftet, die mit dem Carberp-Trojaner etwa 3 Millionen Euro erbeutet haben sollen. Ob die kriminellen Gruppen und deren Festnahmen miteinander in Verbindung stehen, ist unklar.²⁹

Im Oktober 2012 haben Hacker durch DDoS-Attacken die Internet-Auftritte schwedischer Behörden und Banken zeitweise lahmgelegt, u.a. die von Schwedens Zentralbank, des Reichstages, des Polizeigeheimdienstes Säpo, der Staatsanwaltschaft und anderer Behörden. In einem Youtube-Clip im Namen der Hacker-Bewegung Anonymous wurde die großangelegte Aktion angekündigt. Als Begründung wurde dabei unter anderem die Razzia gegen den Webhoster PeRiQuito (PRQ) angegeben, die die schwedische Polizei durchführte. PRQ stellt unter anderem Server für Torrent-Dienste zur Verfügung und war bis vermutlich 2010 auch der Hoster der Whistleblower-Plattform Wikileaks. Diese Polizei-Aktion sei ein „Verbrechen gegen die Informationsfreiheit“ gewesen, so wird im Clip ausgeführt, weshalb aus Protest nun Websites der Regierung und regierungsnaher Organisationen lahmgelegt würden. Die meisten der Betroffenen wie etwa der Geheimdienst Säpo bestätigten die Attacken als Ursache der Störungen. Die Polizei vermutet eine Protest-Aktion gegen die von der schwedischen Regierung geforderte Auslieferung des Wikileaks-Gründers Julian Assange.³⁰ Am 19. März 2013 wurde eine DNS-DDoS-Attacke auf die unabhängige Antispam-Organisation Spamhaus durchgeführt. Dieser Angriff, der auch Spamhaus-Partner in den Vereinigten Staaten, den Niederlanden und Großbritannien betraf, wird von Experten als die bislang heftigste Distributed-DoS-Attacke in der Geschichte des Internet angesehen. Spamhaus hatte zuvor die IP-Adressblöcke des als Spammer-freundlich bekannten niederländischen Hosters Cyberbunker auf seine Blacklist gesetzt. Weil nahezu 80 Prozent aller Antispam-Filter diese Liste einsetzen und damit den Hoster nun blockten, konnten Kunden von Cyberbunker plötzlich kaum noch Mails versenden. Ein 35-jähriger Niederländer, der verdächtigt wird, an

²⁸ Siehe die Stellungnahme des Neiman Marcus unter: http://www.neimanmarcus.com/en-ca/NM/Security-Info/cat49570732/c.cat?icid=topPromo_hmpg_ticker_SecurityInfo_0114

²⁹ <http://www.h-online.com/security/news/item/Carberp-trojan-nets-criminals-almost-Lb170-million-1839746.html>.

³⁰ <http://heise.de/-1724615>.

dem Angriff beteiligt zu sein, wurde in seinem Haus in Barcelona festgenommen. Er soll an die Niederlande ausgeliefert werden und sich dort vor Gericht verantworten.³¹

Im Jahre 2014 gabe es in Deutschland über 32.000 DDoS-Angriffe in nahezu allen Branchen. Ein Viertel der betroffenen Unternehmen war über die Netzinfrastrukturen angegriffen worden.³²

Oft wird Software manipuliert, um schnell an Geld zu gelangen. Im Rahmen eines Ermittlungsverfahrens der Abteilung für organisierte Kriminalität der Staatsanwaltschaft Essen und des Polizeipräsidiums Gelsenkirchen wurden Ende Januar 2015 in mehreren Städten Nordrhein-Westfalens und in fünf weiteren Bundesländern zeitgleich Haftbefehle und Durchsuchungsbeschlüsse vollstreckt. Hintergrund war die professionelle Manipulation der Software von Geldspielgeräten, um Einfluss auf die Gewinnausschüttung zu nehmen. Insgesamt waren 125 Objekte betroffen. Die Schadenssumme ist gleichwohl noch nicht bekannt.³³

Sicherheitslücken werden von Betrügern benutzt, um Dialer in PCs einzuschleusen. Die Hamburger Staatsanwaltschaft hat in einem Fall festgestellt, dass mit Hilfe manipulierter Websites eine international agierende Gruppe einen Trojaner auf dem Rechner des Opfers platzierte. Dieser enthielt einen Dialer, den er im Hauptverzeichnis des Windows-PCs ablegte. Sodann aktivierte er den Dialer und sorgte für eine kurze vom Nutzer unbemerkte Einwahl bei einer Frankfurter Nummer. Anschließend erhielt das Opfer eine Rechnung, mit der es zur Zahlung von 69,95 Euro aufgefordert wurde, wegen der angeblichen Nutzung eines Monats-Abonnements für ein Online-Erotik-Angebot. Mehr als 100.000 Rechnungen sollen von einer Abrechnungsfirma für diesen "Service" versandt worden sein. Auf diese Weise erwirtschafteten die Betrüger bis Mitte 2003 mindestens 1,8 Millionen Euro Umsatz. Der geständige Geschäftsführer der Firma wurde im Juni 2005 zu einer Freiheitsstrafe von einem Jahr auf Bewährung verurteilt.³⁴

Das Internet ermöglicht auch die Verbreitung von Viren. Im Mai 2004 hatte sich der Wurm "Sasser" über Schwachstellen von Betriebssystemen in Rechner eingeschleust. Dadurch schalteten sich die Computer selbstständig ab. Der Wurm verbreitete sich durch das Internet und infizierte weitere Computer. Allein bei der EU-Kommission in Brüssel waren 1200 PCs betroffen. Das Reservierungssystem von Delta Airlines war sieben Stunden außer Betrieb, 40 Flüge mussten annulliert werden. Der Virus "Netsky" attackierte die Computer per Email und störte – unter anderem – Computeranlagen in zwei Bildungseinrichtungen und einer Medizinfirma. Die beiden Viren haben weltweit Computersysteme lahmgelegt, und ihr Programmierer, der zur Tatzeit 17 Jahre alt war, wurde im Juli 2005 vom LG

³¹ <http://www.om.nl/actueel/nieuws-persberichten/@160856/nederlander/>.

³² Die Lage der IT-Sicherheit in Deutschland 2014 S. 21.

³³ <http://www.presseportal.de/blaulicht/pm/51056/2936630#>.

³⁴ <http://www.heise.de/newsticker/Erste-Freiheitsstrafe-wegen-Dialer-Betrugs--/meldung/60377>.

Verden zu einer Jugendstrafe von einem Jahr und neun Monate verurteilt. Die Strafe wurde zur Bewährung ausgesetzt.³⁵

Ende 2013 wurden gefälschte Emails an zahlreiche Internetnutzer geschickt, in denen das BKA als Absender ausgegeben wurde. Der Mail-Betreff lautete "Vorladungstermin Polizei/BKA". "Die Mail-Adresse erweckte den Eindruck, als käme sie vom Bundeskriminalamt". Das sei allerdings nicht der Fall. In der E-Mail gehe es um einen angeblichen Warenbetrug im Internet. Der Empfänger wurde aufgefordert, einen Link anzuklicken, um einerseits mehr über Vorwürfe gegen ihn selbst zu erfahren. Andererseits solle er herausfinden können, ob er selbst Opfer des Warenbetrugs geworden sei.

Der Link führte auf eine Webseite, die unter Umständen Schadsoftware auf dem Rechner installiere – etwa um anschließend Passwörter abzufischen oder den Rechner zu kapern. Das BKA hat den Empfänger geraten, die E-Mail sofort zu löschen,³⁶

In den letzten zehn Jahren hat sich die Zahl jener vermehrt, die die Möglichkeiten des elektronischen Geschäftsverkehrs nutzen. Im Jahr 2004 haben 22,7 Millionen Bürger in Deutschland Waren online – etwa Bücher, Computerspiele, Autos oder Medikamente – gekauft. Ein großer Teil der Internetnutzer informiert sich über Reiseangebote, Telekommunikationsprodukte, Computersoftware und auch über Mode. Deutschland nimmt – nach Angaben einer Studie des "Bundesverbandes Digitale Wirtschaft" – beim Internet-Einkauf den dritten Platz innerhalb der EU-Länder ein.³⁷

Im Jahr 2014 ist der Onlinehandel um knapp 25 Prozent auf 48,8 Milliarden Euro gewachsen. Im Jahr 2013 lag die Wachstumsrate den Zahlen des BVH zufolge bei knapp 42 Prozent, das waren 39,1 Milliarden Euro. Darin sind nicht enthalten digitale Güter wie e-Books, Musik oder Software und Dienstleistungen wie Fahr-scheine, Flugtickets, Reisen und Konzertkarten. Damit wurden noch einmal 10,6 Milliarden Euro Umsatz gemacht. Der Anteil des Versandhandels am gesamten Einzelhandel (ohne Lebensmittel, steuerbereinigt) stieg im Jahr 2013 von 9,4 Prozent auf 11,2 Prozent³⁸

Auch die Kriminellen versuchen, dieses Wachstum zu ihren Gunsten zu missbrauchen. Diese – in den letzten Jahren besonders hervorgetretene – Deliktsgruppe steht in Zusammenhang mit dem elektronischen Handel und stellt – nach einer Statistik des LKA Brandenburg – ein sich sowohl qualitativ als auch quantitativ stark weiterentwickelndes Kriminalitätsfeld dar. In den meisten Fällen bieten die Täter gegen Bargeld über Internetplattformen Waren an, die gar nicht in ihrem Besitz sind. In anderen Fällen versuchen die Täter Waren zu erhalten, ohne

³⁵ Siehe dazu <http://www.dw-world.de/dw/article/0,1564,1644265,00.html>;
<http://w.heise.de/newsticker/Meldung/61416>.

³⁶ <http://www.bsi-fuer-buerger.de/>

³⁷ BVDW, E-Commerce, 2005, S. 9.

³⁸ <http://www.bevh.org/presse/pressemitteilungen/details/datum/2014/februar/artikel/ergebnisse-der-bvh-b2c-studie-2013-liegen-vor-interaktiver-handel-2013-massive-umsatzsteigerungen/?cHash=9ede2a68b8eb6f23ccbe826deff4ae3c>

dafür den entsprechenden Preis zu bezahlen. Oft werden dabei Kontonummern aus weggeworfenen Überweisungsträgern verwendet.³⁹

Eine kriminelle Bande hatte in einem Internet-Auktionshaus fremde Anbieterkonten gehackt und darin nicht existierende Waren wie Elektronikartikel, Computerzubehör, Spiele oder Markenkleidung angeboten. Weit über 1000 Kunden fielen darauf herein. Der Schaden hierbei lag bei 100.000 Euro. Der 34-jährige Drahtzieher der Internet-Hackerbande ist vom Landgericht Bonn wegen Betrugs und Urkundenfälschung in fast 500 Fällen zu sechs Jahren Haft verurteilt worden.⁴⁰

Die elektronischen Plattformen dienen auch als Marktplätze, über die Produktfälschungen angeboten werden. Nach Schätzungen von Experten sind etwa 50% der bei Internetauktionen angebotenen Artikel Fälschungen. Mitte Juni 2005 wurden 14 Wohnungen und Büros in acht deutschen Städten durchsucht. Die Ermittler konnten beweisen, dass eine Gruppe von Kriminellen Luxusartikel der Marke JOOP gefälscht und anschließend über eBay versteigert hatte. Die Einnahmen durch den Verkauf der ca. 76.000 Artikel beliefen sich auf ungefähr 2,3 Millionen Euro. 69 Personen in 27 deutschen Städten sollen beteiligt gewesen sein. Der Kopf der Bande wurde in Istanbul vermutet, von wo aus die Fälschungen nach Deutschland versandt wurden.⁴¹ Anfang Dezember 2014 wurden von EUROPOL 292 Internet Domains beschlagnahmt, die gefälschte Luxusartikel, Sportbekleidung, Elektronikgeräte, Arzneimittel, raubkopierte Filme und Musik verkauften. Obwohl niemand festgenommen wurde, versuchen die Strafverfolger die Geldflüsse nachzuverfolgen.⁴²

Oft wird auch Diebesgut über Online-Marktplätze veräußert, die nach BGH die Straftatbestände der gewerbsmäßigen Hehlerei und des versuchten Betruges erfüllen.⁴³ Außerdem sind Fälle bekannt, in denen ein eBay-Mitglied sein Konto zur Verfügung gestellt hat, damit darüber Diebesgut angeboten werden kann. Auch in solchen Fällen hat der BGH Begünstigung gemäß § 257 Abs. 1 StGB festgestellt.⁴⁴

Nach Angaben der WHO sind 6% der Arzneimittel, die weltweit verkauft werden, Fälschungen.⁴⁵ Nach einer Studie des Europarates steigt die Vermarktung von gefälschten Medikamenten in Deutschland jährlich um 5%.⁴⁶ Dass der Online-Versand hier eine wichtige Rolle spielt, liegt auf der Hand. Ende Juli 2005 hat sich im Zuge eines staatsanwaltlichen Ermittlungsverfahrens in Saarbrücken heraus-

³⁹ Pressemitteilung des LKA Brandenburg v. 18.4.2005.

⁴⁰ <http://www.datenschutzticker.de/index.php/2013/03/landgericht-bonn-sechs-jahre-haft-fuer-internet-hackerbanden-chef/>

⁴¹ Dazu <http://www.onlinemarktplatz.de/modules.php?name=News&file=article&sid=1314>.

⁴² <https://www.europol.europa.eu/content/292-internet-domain-names-seized-selling-counterfeit-products>

⁴³ S. BGH, 27.8.2008 – 2 StR 329-08, MMR 208, 728 f.

⁴⁴ BGH, 29.4.2008 – 4 StR 148/08, KJR 208, 533, s. dazu auch Schlömer/Dittrich, KJR 2009, S. 147.

⁴⁵ <http://www.who.int/medicines/organization/qsm/activities/qualityassurance/cft/CounterfeitOverview.htm>

⁴⁶ Council of Europe, Counterfeit Medicines, Survey Report, S. 27.

gestellt, dass auf Internetbestellung teure gefälschte Medikamente versandt wurden, die entweder völlig wirkungslos oder gesundheitsgefährdend waren.⁴⁷

Die Nutzung des Internet für "day-to-day-business" hat in den letzten sieben Jahren einen neuen Tätigkeitsbereich für Kriminelle eröffnet. Die "Cyber-Umgebung" ist in solchen Fällen nicht selbst das Ziel von Angriffen. Die Kriminellen missbrauchen sie nur, um Straftaten vorzubereiten oder diese in ein Versuchsstadium zu bringen. Es handelt sich dabei um die Konstellation, in der das Internet als "Tatmittel" benutzt wird.

Ein Beispiel für den Missbrauch der "Cyber-Umgebung" ist die Zusendung von "Spam". Nach Angaben der OECD handelt es sich bei der Hälfte allen E-Mail-Verkehrs um Spam.⁴⁸ Es wird geschätzt, dass im Jahre 2003 4,9 Trilliarden Spammails gesendet wurden;⁴⁹ allein AOL gibt an, dass im April 2003 2,37 Billionen Spammails pro Tag abgeblockt wurden.⁵⁰ Die Firma Brightmail, ein Entwickler von Softwarefiltern, prüfte im Jahr 2004 über 106 Milliarden Spammails aus der Internetkommunikation und stellte fest, dass die meisten Spammails Produkte oder Dienstleistungen anbieten.⁵¹ Es folgen Dienstleistungen für Erwachsene und die sog. Nigeria-E-Mails.⁵² Im Juli 2009 wurde 89% aller E-Mails als Spam registriert.⁵³

Die Spam-Flut hat Firmen in Europa im Jahr 2002 \$ 2,5 Milliarden und in der USA im Jahr 2003 \$ 10 Milliarden gekostet. Faktoren die hier berechnet wurden, waren:

- die Zeit, die von den Arbeitnehmern verwendet wird, um die Werbe-E-Mails zu checken und auszusortieren,
- die Kosten, die durch die zusätzlichen Computer- und Netzwerkressourcen entstehen, die für die Bewerksstellung von Werbe-E-Mails erforderlich sind, und
- die finanziellen Investitionen in technische Maßnahmen wie Filter und in Arbeitsleistungen, die sich mit der Abwehr von Angriffen durch Werbe-E-Mails beschäftigen.⁵⁴

⁴⁷ Dazu <http://www.justiz-spzoales.saarland.de/detail.htm?mid=7884>.

⁴⁸ Siehe dazu OECD, Background Paper for the OECD Workshop on Spam, S. 4.

⁴⁹ *Gauthroner/Drouard*, Unsolicited Commercial Communications and Data Protection S. 67.

⁵⁰ *Krim*, Spam Cost to Business Escalates, Washington Post v. 13.3.2003.

⁵¹ Siehe die detaillierte Darstellung in: Brightmail's Prove Network, The State of Spam – Impact and Solutions.

⁵² Nigeria-E-Mails sind E-Mails, die dem Empfänger eine große Geldsumme versprechen, wenn er z. B. afrikanischen Geschäftsleuten, einer Diktatorenwitwe oder einem verschollenen Prinzen helfen würde, riesige Beträge – regelmäßig Millionen Dollar – außer Landes zu schaffen. Der E-Mail-Empfänger soll nach dem Inhalt der E-Mail – sein Konto kurzfristig zur Verfügung stellen, um die Millionen für kurze Zeit "zu parken". Geht der Internetnutzer auf diese E-Mail ein, dann wird eine "geringe Gebühr" für das gewinnbringende Geschäft verlangt, z. B. für Überweisungen, Anwaltskosten oder Steuern, die oft einige tausend Dollar hoch sein können. Dass die versprochenen Millionen nie ausgezahlt werden, versteht sich von selbst.

⁵³ S. Symantec, Spam Report, August 2009, S. 4.

⁵⁴ Siehe dazu *Krim*, Spam Cost to Business Escalates, Washington Post, 13.3.2003.

In seinem Spam-Bericht für September stellte Kaspersky fest, dass Deutsche Internet-Nutzer weltweit die meisten schädlichen Anhänge und Links in ihren Postfächern vorfanden und lösten damit die USA an der Spitze ab. Neben dem höheren Aufkommen an gefährlichem Spam haben sich die Methoden verändert: Die Absender geben sich politischer.⁵⁵

Auch die Android-Betriebssysteme sind vom Spam betroffen. In den USA breitet sich ein neues Botnetz für solche Systeme namens Spamsoldier aus. Das Botnetz verbreitet sich durch SMS, die Gratisversionen von Spielen wie Need for Speed oder Angry Birds Space versprechen. In der SMS werden die Spiele über Links zum Download angeboten. Sobald ein Nutzer dem Link folgt, installiert sich der als App getarnte Trojaner – teilweise werden auch wirklich Gratisspiele zur Ablenkung des Nutzers mitgeliefert. Der Trojaner nimmt dann Kontakt mit einem Command-and-Control-Server auf. Dieser schickt Spamsoldier eine Liste von 100 Mobilfunk-Rufnummern in den USA und eine passende Spam-SMS, die der Bot nun – so schnell es das Mobiltelefon erlaubt – an die Liste schickt. Sind die 100 Nummern abgearbeitet, lässt sich die Schadsoftware neue Listen vom C&C-Server schicken, bis dieser nicht mehr antwortet oder neue Befehle gibt. Seine Aktivität versucht der Trojaner kontinuierlich zu verschleiern. Alle ausgehenden Spam-SMS werden gelöscht. Antwortende SMS auf den Spam versucht das Programm ebenfalls zu entfernen.⁵⁶

Das Bundesamt für Sicherheit in der Informationstechnik hat in seiner Zusammenfassung der IT-Sicherheitslage in Deutschland festgestellt, dass sich im Jahr 2014 bezüglich der Spam-Zahl mit einem deutlichen Zuwachs von ca. 80% im Vergleich zum Vorjahr eine Trendwende bei den seit Jahren stagnierenden Zahlen abzeichnet.⁵⁷

Eine andere Missbrauchsform der Cyber-Umgebung ist die Zusendung von "Phishing-Mails", nämlich der Versuch der Entwendung vertraulicher Daten von Internet-Nutzern – z. B. Kreditkartennummern, Bankverbindungen, TAN oder PIN. Nach Angaben der "Anti-Phishing-Working-Group" ist ein Zuwachs an Vorfällen bis zu monatlich 24% festzustellen.⁵⁸ Nach dem Phishing Activity Report, von Juli 2005 haben 85,9% der "Phishing-Mails" als Ziel die Erlangung von Online-Banking-Zugangsdaten.⁵⁹ Man hat errechnet, dass im Jahr 2003 den Finanzdienstleistern und Kreditkarteninhabern durch Phishing Schäden in Höhe von \$ 1,2 Milliarden entstanden sind.⁶⁰ Im Jahr 2007 ist die Zahl der Phishing-Fälle bei Onlinebanking gestiegen. Bundesweit hoben Kriminelle in mehr als 4 100 Fällen rd. € 10 Mio. von Konten der Geschädigten ab. Die Schadenssumme liegt um ein Viertel höher als 2006. Auch in-

⁵⁵ Kaspersky lab, Spam im September 2012

⁵⁶ <https://blog.lookout.com/blog/2012/12/17/security-alert-spamsoldier/>

⁵⁷ Die Lage der IT-Sicherheit im Deutschland 2014, S. 15:

⁵⁸ S. www.antiphishing.org.

⁵⁹ Phishing Activity Report, July 2005, S. 2.

⁶⁰ Gartner, Phishing Victims Likely Will Suffer Identity Theft Fraud, S. 5.

ternational haben die Phishing-Betrugsversuche zugenommen. Die APWG registrierte in ihrer Statistik vom Dezember 2007 weltweit über 25 000 Attacken pro Monat.⁶¹

Wie der Präsident des Bundeskriminalamtes (BKA), Jörg Ziercke mitteilte, lag 2006 die Schadenshöhe aus den Phishing-Fällen im Durchschnitt noch bei 2500 Euro, während im Jahr 2008 es schon 4000 bis 4500 Euro pro Fall waren. „Nach Schätzungen waren im Jahr 2008 mehr als 750 000 Computer in Deutschland mit Schadprogrammen infiziert, etwa 150 000 Rechner werden von Kriminellen unbemerkt ferngesteuert.“⁶²

Auch Microsoft wurde Opfer von Phishing-Attacken. Im Rahmen von Phishing-Attacken auf E-Mail- und Social-Media-Konten von Mitarbeitern des Konzerns Anfang des Jahres sind auch sensible Daten zu Anfragen von Polizeibehörden abhandengekommen. Nach Angaben des Konzerns seien die Vorgänge dem derzeitigen Informationsstand nach Teil der Angriffe der Syrian Electronic Army gewesen. Die Aktivistengruppe, die dem Assad-Regime nahestehen soll, hatte Anfang des Jahres mehrfach Blogs von Microsoft verändert und angekündigt Internet-Konten von Microsoft-Angestellten gehackt.⁶³

Über Phishing-Attacken haben Cyberkriminelle sich Zugriff auf Computer von Angestellten einer ukrainischen Bank verschafft und diese mit einem Schadprogramm infiziert. Dadurch kontrollierten sie Überwachungskameras und Geldtransfersysteme. Auf diese Weise manipulierten sie die Buchhaltungssysteme vieler Banken, erhöhten die Kontosaldis und überwiesen anschließend die Differenzbeträge auf Konten in China oder in die USA. Von dort wurde das Geld dann durch kontrollierte Geldautomaten an die Täter ausgezahlt. Der Schaden wurde auf 1 Milliarde \$ geschätzt. Laut Europol und Interpol ist dieser Fall der größte bekanntgewordene Cyber-Bankraubüberfall, in dem bis zu 100 Geldinstitute in über 20 Ländern angegriffen wurden. Die Täter begannen mit ihren Vorbereitungen Ende 2013, bis sie Anfang 2015 aufgedeckt wurden.⁶⁴

Oft wird Erpressungs-Malware automatisch eingesetzt. Die Antivirenexperten von Trend Micro haben einen Lösegeld-Trojaner entdeckt, der den Boot-Vorgang blockiert. Der Schädling führt einen Neustart durch und fordert den Nutzer auf, ein Lösegeld in Höhe von 920 Hrywnja (ukrainische Währung, umgerechnet rund 90 Euro) über den Zahlungsdienstleister QIWI an die Erpresser zu zahlen.⁶⁵

Das Landgericht Gießen hat Ende Juni 2014 fünf junge Männer aus Mecklenburg-Vorpommern und drei weiteren Bundesländern schuldig gesprochen, bundesweit mehr als 40 Online-Shops lahmgelegt und deren Betreiber erpresst zu haben. Die

⁶¹ S. MMR Aktuell, XVI MMR 10/2008.

⁶² Neue Osnabrücker Zeitung v.15.3.2008.

⁶³ <http://www.securityweek.com/hackers-steal-law-enforcement-inquiry-documents-microsoft>

⁶⁴ <http://newsroom.kaspersky.eu/de/texte/detail/article/der-grosse-bankraub-cybergang-carbanak-stiehlt-eine-milliarde-us-dollar-von-100-finanzinstitut>.

⁶⁵ Siehe Malware blockiert Bootvorgang, Heise 13.4.2012.

Richter erkannten unter anderem auf Computersabotage und Erpressung. Einer der Angeklagten erhielt ein Jahr und zehn Monate Haft auf Bewährung, die übrigen wurden nach Jugendstrafrecht verurteilt und erhielten bis zu eineinhalb Jahren auf Bewährung. Die Täter hatten die Shops zwischen 2010 und 2011 attackiert und mit unzähligen Anfragen die Server der Firmen lahmgelegt. Danach forderten sie von den Betreibern 100 bis 350 Euro, damit sie die Angriffe beenden. Allerdings ging nur ein kleiner Teil darauf ein. Die Umsatzeinbußen der Shop-Betreiber sollen im sechsstelligen Bereich liegen.⁶⁶

US-Hacker behaupteten, sich über die Server der Finanzprüfer PriceWaterhouseCoopers Zugriff auf die Steuerunterlagen von Mitt Romney verschafft zu haben, dem Präsidentschaftskandidaten der Republikaner 2012. Die Hacker wollten verschlüsselte Kopien der Unterlagen an zahlreiche US-Medien verschickt haben und drohten mit der Freigabe der Schlüssel. Der wegen seines Steuersatzes von 13 Prozent oftmals kritisierte Romney könne die Veröffentlichung aber mit einem Schweigegeld verhindern – in Höhe von einer Million Dollar. Ob die Hacker tatsächlich brisantes Material in Händen gehalten haben, ist noch unklar. Der Secret Service soll Ermittlungen in der Sache angestellt haben. PriceWaterhouseCoopers teilte mit, keinen Hinweis auf einen Einbruch in das eigene Computersystem gefunden zu haben.⁶⁷ Im März 2013 warnte der BKA vor einer neuen Variante des BKA-Trojaners, die den Rechner von betroffenen Computeranwendern sperrt und eine Art Lösegeld einfordert. Ähnlich wie bei einer früheren Variante, erscheint, wenn der Rechner infiziert ist, auf dem Bildschirm ein nicht wegzuklickendes Fenster. Diesem wird durch Anzeige des Logos der BKA-Pressestelle ein vermeintlich offizieller Anstrich gegeben, erklärte das Bundeskriminalamt. Dabei werde behauptet, dass die Funktion des Computers "aus Gründen unbefugter Netzaktivitäten ausgesetzt" sei. Außerdem werden Rechtsverletzungen angeführt, die die vermeintliche Ursache für die Sperrung sein sollen. Bei der aktuellen Variante der Schadsoftware werden vier Fotos eingeblendet. Dabei handelt es sich um eine strafbewehrte jugendpornografische Darstellung. Im weiteren Text wird behauptet, dass "die Wiedergabe von pornografischen Inhalten mit Minderjährigen festgestellt" worden sei. Der Nutzer werde aufgefordert, 100 Euro über die Zahlungsdienstleister uKash oder Paysafecard zu zahlen, um einen Freigabecode zur angeblichen Entsperrung des Rechners zu erhalten. Gleichwohl ist der Rechner in diesem Fall schon infiziert und wird auch durch eine Zahlung des Lösegelds nicht wieder sauber.⁶⁸

Der Erpressungs-Trojaner Bitcrypt verschlüsselte Dateien des Anwenders und gab sie nur gegen Zahlung von 260 Euro Lösegeld frei. Nach der Überweisung haben die Erpresser dem Anwender das zugehörige Entschlüsselungsprogramm

⁶⁶ Dazu siehe:
http://www.hr-online.de/website/rubriken/nachrichten/indexhessen34938.jsp?rubrik=36090&key=standard_document_52202697&tl=rs

⁶⁷ <http://h-online.com/-1702616>

⁶⁸ http://www.bka.de/nn_233148/DE/Presse/Pressemitteilungen/Presse2013/130322__Warnmeldung__Ransomware.html

gesendet, das die Daten wieder dechiffrieren ließ. Sicherheitsexperten haben jedoch das Programm geknackt und das profitabel Geschäft gestoppt.⁶⁹

Im Dezember 2014 haben Online-Erpresser Kryptofunktionen in eine Web-Anwendung eines europäischen Finanzdienstleisters gebaut und verschlüsselten alle Daten, die in der Datenbank gespeichert waren. Anschließend forderten die Täter Lösegeld in Höhe von 50.000 \$.⁷⁰

Insgesamt haben Cyberkriminelle durch Erpressungs-Software von April 2014 bis Juni 2015 – laut Angaben des FBI – 18 Millionen \$ erpresst. Die Lösegeld-Transfers erfolgten meist über Bitcoin, die Mittelsmänner entgegennahmen und dann über ihre Bankkonten oder Transferdienste wie Western Union überwiesen.⁷¹

In ihrer Studie «Bedrohungen 2012» hat die Sicherheitsfirma McAfee betont, dass die Angriffe gegen industrielle Steuerungssysteme zunehmen werden. Die Studie berichtet vor allem über das Problem der "eingebetteten Hardware", nämlich über die produktiven Komponenten, die mit üblichen informationsverarbeitenden Komponenten vernetzt sind. Diese Malware ist in der Lage, die Steuerungen für industrielle Fertigungsanlagen anzugreifen.⁷²

Im Oktober 2012 ist die US-amerikanische Federal Trade Commission (FTC) zusammen mit Kollegen aus fünf Ländern (Kanada, Australien, Irland, Neuseeland und Großbritannien) gemeinsam gegen eine Reihe von Telefon-Scammern vorgegangen. Den Beschuldigten wird vorgeworfen, zehntausenden Computernutzern vorgetäuscht zu haben, dass ihr Rechner von Malware befallen sei. Die Beschuldigten sollen ihre Herkunft verschleiert haben, indem sie Briefkastenfirmen unterhielten, 80 verschiedene Domains und 130 Rufnummern nutzten. Sie sollen sich betrügerisch als Anrufer im Auftrag eines renommierten Unternehmens wie Microsoft, Dell oder McAfee ausgegeben und bereitwillige Windows-Nutzer am Telefon zum Ereignisprotokoll ihres Betriebssystems gelotst haben. Anhand der dort aufgeführten möglichen gewöhnlichen Fehler- und Warnhinweise wurde den Nutzern suggeriert, dass ihr Computer mit Malware infiziert sei. Die Betrüger hätten gegen einen Betrag von 50 bis zu 450 US-Dollar angeboten, die vermeintliche Infektion zu beseitigen. Dafür sollten die Nutzer eine Software herunterladen, die angeblich die Malware beseitigt. Über diese Software hatten die Betrüger dann stattdessen Fernzugriff auf die Rechner der Betroffenen gewonnen und konnten so Software auf die betroffenen Rechner laden. In anderen Fällen hat eine betrügerische Firma auf Google Anzeigen geschaltet, die die vermeintliche Rufnummer des Supports eines IT-Unternehmens anzeigte. Verdächtige Unternehmen in Indien seien direkt nicht anzugehen gewesen; wenn diese aber US-Telefonunternehmen für ihre Machenschaften genutzt hätten, seien die Ruf-

⁶⁹ <http://blog.cassidiancybersecurity.com/post/2014/02/Bitcrypt-broken>

⁷⁰ https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html.

⁷¹ <http://www.ic3.gov/media/2015/150623.aspx>.

⁷² McAfee, Bedrohungen 2012, 2012.

nummern von den Unternehmen blockiert worden. Die australische Behörde Australia Communication and Media Authority (ACMA) schildert, tausende Telefonkunden, die sich in das Register "Do not call" eingetragen hatten, hätten sich seit 2009 vermehrt über Anrufe beschwert. Diesen Fällen sei die ACMA nachgegangen und habe diese an die FTC weitergeleitet. Australien gehörte demnach zu den ersten Zielen der Telefon-Scammer.⁷³

Die Malware wird auch für Zwecke der Industriespionage eingesetzt. Das Ziel ist Knowhow des Konkurrenten anzupapfen, um so Entwicklungskosten zu sparen und ähnliche Produkte schnell und günstig auf den Markt zu bringen. Nach der neuen Studie von Corporate Trust "Industriespionage 2012" entsteht der deutschen Wirtschaft durch Industriespionage jährlich ein Gesamtschaden von ca. 4,2 Milliarden Euro. Es wurden Daten von circa 600 vorwiegend mittelständischen Unternehmen erhoben, die belegen, dass das Bedrohungspotential durch kriminelle Handlungen im Internet in den vergangenen Jahren um 50 % gestiegen ist.⁷⁴

Die sog. Cyberspionage-Kampagne horcht seit 2004 systematisch bis zu 1000 Personen aus mindestens 40 Ländern aus. 350 der ausspionierten Personen, die identifiziert werden könnten, bekleiden wichtige Positionen in privaten und öffentlichen Einrichtungen, Regierungsinstitutionen, Forschungseinrichtungen oder der Rüstungsindustrie. Außerdem wurden auch Tibet-Aktivisten angegriffen. Die als NetTraveler benannte Kampagne beschaffte sich so vor allem Informationen aus den Bereichen der Weltraumforschung, Nanotechnologie, Energieproduktion, Nuklearenergie, Lasertechnologie, Medizin und Kommunikation. Die Opfer infizierten sich mit der Spionagesoftware über gezieltes Phishing (Spear Phishing). Von den 350 identifizierten Opfern in 40 Ländern kommen die meisten – der Anzahl nach geordnet – aus der Mongolei, Russland, Indien, Kasachstan, Kirgisistan, China, Tadschikistan, Südkorea, Spanien und Deutschland. Deutschland hat es so in die Top 10 der am meisten betroffenen Nationen geschafft.⁷⁵

Malware ist nicht leicht zu entdecken. Die "The Mask" getaufte Malware-Kampagne lief seit mindestens 2007. Die von Kaspersky-Forschern entdeckte und analysierte Kampagne hat über 400 Maschinen in 31 Staaten infiziert, darunter drei in Deutschland. Ziel der Attacken waren vor allem Regierungsbehörden, Büros von Diplomaten und Botschaften, Energie-, Öl- und Gasunternehmen, Forschungseinrichtungen und Aktivisten. Die Schadsoftware saugte alle möglichen Dateien von den infizierten Rechnern ab, darunter Office-Dokumente, Private Keys zum Signieren von PDFs, VPN-Konfigurationsdateien, PGP-Keys, SSH-Schlüssel oder Dateien zur Konfiguration von RDP (Remote Desktop Client). Auch Skype-Telefonate und Tastatureingaben seien mitgeschnitten und bombensicher verschlüsselt auf dem Command & Control-Server abgelegt worden. Von der professionellen Operation gibt es im Netz keine Spur mehr: Vier Stunden nachdem

⁷³ <http://ftc.gov/opa/2012/10/pecon.shtm>, FTC Halts Massive Tech Support Scams

⁷⁴ Siehe Corporate Trust, Studie Industriespionage 2012.

⁷⁵ The Nettraveler, Kaspersky Lab.

Kaspersky per Blogbeitrag eine Aufsehen erregende Analyse ankündigte, waren sämtliche zu The Mask gehörende Server aus dem Netz verschwunden.⁷⁶

Nach einem Dossier der US-amerikanischen Geheimdienste (National Intelligence Estimate, NIE) sind die USA das Ziel einer "massiven und anhaltenden Cyber-Spionage-Kampagne". Neben China sollen Russland, Israel und Frankreich zu den Ländern gehören, die durch Hackerangriffe gegen die USA aufgefallen sein sollen. Dabei gehe es um Wirtschafts- und Militärspionage.⁷⁷

Die Gesamtzahl der Malware übersteigt – Schätzungen zufolge – die 250-Millionen-Marke während ihre Zahl täglich um rund 300.000 steigt.⁷⁸

Mit Malware und Social-Engineering hat eine internationale Bande E-Mail-Systeme mittlerer und größerer europäischer Firmen gehackt und ist in deren Computernetzwerke eingebrochen. Dann wurden die Zahlungsforderungen an diese Firmen gefälscht und die Bankkonten der Täter angegeben. Der Schaden der Unternehmen wurde um die 6 Millionen Euro geschätzt. Die Bande war nach Angaben von Europol, die Mitte Juni 2015 49 Verdächtige verhaftet und 58 Häuser durchsucht hatte, in Italien, Spanien, Polen, Großbritannien, Belgien und Georgien aktiv. Die meisten Verdächtigen, die nach Polizeiangaben aus Nigeria, Kamerun und Spanien kommen, haben ein Geldwäsche-Netzwerk gebildet.⁷⁹

2 Delikte gegen den demokratischen Rechtsstaat

Strafrechtliche Urteile und Berichte des Bundesamtes für Verfassungsschutz weisen darauf hin, dass die neuen Technologien bzw. das Internet von Extremisten genutzt werden.⁸⁰ Die extremistischen Angebote rufen oft zu gewalttätigen Aktionen gegen Minderheiten oder staatliche Einrichtungen auf oder stellen das demokratische System in Frage. Das Internet fördert die Verbreitung von Propagandamaterial, die Werbung von Mitgliedern verbotener Organisationen oder die rasche Information über spontane Operationen.⁸¹ Nach Angaben des Verfassungsschutzberichts 2004 ist die Nutzung des Internet für deutsche Rechtsextremisten zur Selbstverständlichkeit geworden. Sie verbreiten ihre Propaganda durch von ihnen betriebene Webseiten und verwenden Internetdienste, um ihre

⁷⁶ Dazu Kaspersky Lab, Unveiling Careto – The Masked APT, February 2014

⁷⁷ http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html

⁷⁸ Die Lage der IT-Sicherheit in Deutschland 2014, S. 26.

⁷⁹ <https://www.europol.europa.eu/content/international-operation-dismantles-criminal-group-cyber-fraudsters-0>

⁸⁰ Siehe dazu etwa BGH v. 12.12.2000, 1. StR. 184/00, NJW 2001, 624; AG Tiergarten CR 1998, m. Anm. Vassilaki, S. 111 f.; Bundesministerium des Innern, Verfassungsschutzbericht 1997; Bundesamt für Verfassungsschutz 1997, Extremistische Bestrebungen im Internet, 1998; Verfassungsschutzbericht 2002, S. 103 f.; Verfassungsschutzbericht 2003, S. 107.

⁸¹ So sind etwa – nach Angaben der Tageszeitung v. 25.6.1998, 21 – Straftaten randalierender deutscher Hooligans während der Fußball-WM 1998 in Frankreich über das Internet verabredet worden.

verfassungswidrigen Weltanschauungen bekannt zu machen. Die Zahl der deutschen rechtsextremistischen Homepages belief sich 2002 auf 1.000, sie ist 2003 und 2004 allerdings leicht gesunken und erreichte die Zahl 950.⁸²

Der Tätigkeitsbericht 2003 der Internet-Meldestelle "netwatch" meldet, dass im Jahr 2003 570 Beanstandungen eingegangen sind, die den Problembereich "Rechtsextremismus" betrafen. Dabei wird betont, dass für diesen Themenbereich und für den Bereich Kinderpornographie die meisten Beanstandungen im Jahr 2003 eingingen.⁸³ Gleichwohl stieg in der letzten Zeit die Anzahl der Fälle des Rechtsextremismus, in denen das Internet für dessen Zwecke benutzt wurde. Am 14.6.2012 meldete das BKA, dass im Auftrag des StA Rostock Beamte des BKA in Kooperation mit der Polizei und Spezialkräften der Bundespolizei in 11 Bundesländern Durchsuchungsmaßnahmen gegen die Betreiber des rechtsextremen «Thiazi»-Forums wegen des Verdachts der Bildung einer kriminellen Vereinigung durchgeführt haben. Die Betreiber bezeichneten das Forum als "germanische Weltnetzgemeinschaft" und verstanden dieses als "das größte und bekannteste deutschsprachige Forum seiner Art" mit weit über einer Million Foren-Beiträgen. Die 26 Beschuldigten im Alter von 22 bis 64 Jahren aus dem gesamten Bundesgebiet sind verdächtig, mehr als 2.400 Liedtexte von Tonträgern und mehr als 1.400 Tonträger zum Download angeboten zu haben. In einer Vielzahl der Liedtexte wird zum Hass gegen Ausländer, Juden und Menschen anderer Hautfarbe aufgestachelt und zu gewalttätigen Übergriffen gegen diese aufgerufen. Ferner werden die genannten Personengruppen in menschenverachtender Weise beschimpft, der Holocaust geleugnet und die nationalsozialistische Gewalt- und Willkürherrschaft verherrlicht. Entsprechende Inhalte finden sich auch in anderen Bereichen des Forums.⁸⁴

Das Anbieten von verbotenen NS-Symbolen, Spielen, Musik und volksverhetzenden Texten soll Jugendliche ansprechen und neue Mitglieder anwerben. Zugleich werden Internetdienste dazu verwendet, um eine große Zahl von Rechtsextremisten für Aktivitäten – etwa Demonstrationen, Kundgebungen, Lynchjustiz,⁸⁵ oder Mahnwachen – zu mobilisieren.

Unter diesem Gesichtspunkt ermöglichen die entsprechenden Handlungen die Begehung von Delikten, die sich gegen den demokratischen Rechtsstaat richten, wie etwa Volksverhetzung nach § 130 StGB, die Anleitung zu Straftaten gem. § 130a StGB oder die öffentliche Billigung von Straftaten gem. § 140 Nr. 2 StGB.

Eine andere Angriffsform gegen den demokratischen Rechtsstaat ist der sog. „Cyberwar“. Darunter versteht man Angriffe gegen militärische Infrastrukturen für Spionage-, Sabotage- und Manipulationszwecke. Der militärische Hacker attackiert jede Variante der IT-Sicherheit und nutzt dafür die Vernetzung. Er führt Operationen un-

⁸² Vgl. dazu Verfassungsschutzbericht 2004, 115.

⁸³ Siehe Netwatch, Tätigkeitsbericht 2003, S. 3.

⁸⁴ S. Pressestelle des BKA v. 14.6.2012.

⁸⁵ Ostendorf/Frahm/Doege, NSStZ 2012, S. 529.

abhängig von konkreten Konflikten, um einen Gegner langfristig zu schwächen. Dafür wird spezielle Software verwendet. Als Beispiel dafür sei „Stuxnet“ erwähnt. Stuxnet ist ein Computerwurm, der im Juni 2010 entdeckt und in seiner Ursprungsform speziell für ein bestimmtes System zur Überwachung und Steuerung technischer Prozesse (SCADA-System) der Firma Siemens, die Simatic S7, entwickelt wurde. Die Angriffe der Software gegen die Steuerung von Frequenzumrichtern der Hersteller *Vacon* aus Finnland und *Fararo Paya* in Teheran oder der Einsatz von Frequenzumrichtern, um die Geschwindigkeit von anderen Geräten wie beispielweise Motoren zu steuern, und ihre technische Besonderheiten lassen vermuten, dass das Programm als Waffe gegen militärische Ziele entwickelt wurde.⁸⁶

In Deutschland haben Verfassungsschützer im Jahr 2012 mehr als 1000 Angriffe chinesischer Hacker auf Computer deutscher Bundesbehörden und fast 1100 digitale Angriffe ausländischer Nachrichtendienste registriert. Hinzu kämen Ausspähaktionen in deutschen Unternehmen. Ebenfalls 2012 wurde eine bemerkenswerte Attacke auf die Rechner des Luft- und Raumfahrtkonzerns EADS registriert. Der Vorgang sei nach Angaben aus Unternehmenskreisen so gravierend gewesen, dass EADS ihn der Bundesregierung gemeldet habe. Auch ThyssenKrupp beklagte Mitte 2012 Angriffe, die "massiv" waren und "eine besondere Qualität" hatten. Die Attacke sei "in den USA" erfolgt; die Adressen der Täter seien chinesisch. Genauere Erkenntnisse über mögliche Schäden der Angriffe gab es nicht.⁸⁷

Im März 2013 gab die australische Zentralbank an, Ziel von Cyberattacken gewesen zu sein. Die Hacker wollten offenbar Informationen zu G20-Verhandlungen bei der Zentral-Bank erbeuten. Die Angreifer sollen dabei in China entwickelte Malware verwendet haben und tatsächlich an vertrauliche Informationen gelangt sein. Die australische Zentralbank bestätigte allerdings in ihrer Mitteilung weder die mutmaßlich chinesische Malware noch einen G20-Bezug der Angriffe.⁸⁸

Mitte November 2014 wurde das US-Außenministerium Ziel eines Hackerangriffs. Obwohl das interne E-Mail System und die Webseite vorübergehend vom Netz genommen wurden, sagte der Regierungssprecher, dass keine vertraulichen Systeme getroffen worden seien.⁸⁹ Auch abgeschottete Netzwerke lassen sich mittels elektromagnetischer Wellen infiltrieren. Die US-Army betreibt ein "Tactical Electromagnetic Cyber Warfare Demonstrator"-Programm, in dem es unter anderem darum geht, Daten aus abgeschotteten Kabelnetzwerken nicht nur zu extrahieren, sondern dort auch einzuschleusen. So wäre es etwa möglich, einen Spionagetrojaner einzuschleusen, indem man kurze Zeit ein Fahrzeug vor dem Gebäude parkt, in dem

⁸⁶ Siehe dazu auch für Stuxnet <http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1/view?searchterm=None>, im Allgemeinen zur Cyberwar: *Gaycken/Karger*, MMR 2011, S. 3 ff.

⁸⁷ http://www.business-on.de/weser-ems/politik-und-wirtschaft-hacker-nehmen-offenbar-deutschland-aufs-korn-_id28812.html.

⁸⁸ <http://www.rba.gov.au/media-releases/2013/mr-13-05.html>

⁸⁹ http://www.nytimes.com/2014/11/17/us/politics/state-department-targeted-by-hackers-in-4th-agency-computer-breach.html?ref=technology&_r=1.

das zu infiltrierende Netz betrieben wird. Die Urananreicherungsanlage im iranischen Natanz könnte etwa durch einen speziell präparierten USB-Stick mit dem destruktiven Stuxnet-Wurm infiziert worden sein. Das Einschleusen über elektromagnetische Strahlen wäre daher eine willkommene Alternative – nicht nur für US-Behörden. Dass sich die elektromagnetische Abstrahlung elektronischer Geräte zur Spionage eignet, ist freilich nicht neu – die NSA forscht unter dem Codenamen TEMPEST bereits seit Jahrzehnten daran. Das Prinzip beruht darauf, dass die Kabel elektronischer Geräte prinzipiell auch als Antennen arbeiten, welche die übertragenen Daten ausstrahlen. Auf diese Weise wurden etwa bereits Lauschangriffe auf Tastaturen und Monitore demonstriert.⁹⁰

Nach einem Bericht des Kaspersky Labs wurden seit geschätzten fünf Jahren Rechnernetzwerke von diplomatischen Vertretungen, Regierungs- und Handelsorganisationen, Energie-Konzernen sowie Einrichtungen der Forschung, der Luftfahrt und des Militärs infiltriert. Über eine ausgeklügelte Infrastruktur konnten die unbekanntesten Hacker vermutlich Terabyte an geopolitischen Information und Daten höchster Vertraulichkeit erbeuten. Betroffen von der umfassenden Spionage waren hauptsächlich Organisationen aus osteuropäischen und zentralasiatischen Ländern ebenso wie aus den ehemaligen Sowjet-Republiken, wobei Russland die höchste Zahl an Infektionen aufwies, gefolgt von Kasachstan und Aserbaidschan. Westeuropäische und nordamerikanische Institutionen sollen nur im geringen Umfang ausspioniert worden sein. Um die Infektionen einzuleiten, haben die Hacker offenbar "Spear Phishing" betrieben. Ausgewählten Opfern wurden E-Mails mit angehängten infizierten Dokumenten zugesickt, wobei die Dokumente möglichst interessant für die jeweilige Zielperson gestaltet wurden. Nach erfolgter Infektion mit der Hauptkomponente der Malware wurden dann über die C&C-Server unbemerkt weitere Module heruntergeladen, zum Beispiel zur Infektion des Smartphones des Opfers. Unter anderem wurden zur Infektion Sicherheitslücken in MS Word, MS Excel und im Adobe Reader ausgenutzt. Auch Dateien von USB-Speichermedien konnten erbeutet werden, einschließlich gelöschter Daten, die „Roter Oktober“ offenbar über eine eigene Recovery-Prozedur wiederherstellen kann.⁹¹

3 Delikte gegen die Persönlichkeit i.w.S.

Die Anonymität der Kommunikation via Internet erleichtert jede Art von Verletzungen, die als Ziel die Persönlichkeit der Mediennutzer haben. Oft erscheinen E-Mails oder Nachrichten mit ehrverletzendem Charakter, für die eine Strafbarkeit gem. §§ 185-186 StGB in Betracht kommt.⁹²

⁹⁰ <http://www.defensenews.com/article/20130115/C4ISR01/301150010/DoD-Looking-8216-Jump-Gap-8217-Into-Adversaries-8217-Closed-Networks?odyssey=nav%7Chead>.

⁹¹ http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies.

⁹² Siehe dazu etwa LG Hamburg CR 1998, 565, das den Beklagten wegen Verletzung des Persönlichkeitsrechts zur Schadensersatzleistung verurteilt hatte.

Darüber hinaus ermöglicht die Nutzung der neuen Kommunikationstechniken die Sammlung von personenbezogenen Daten, die etwa zu Abrechnungs- oder Werbezwecken verwendet werden. Diese persönlichen Daten bilden ein wertvolles Kapital, das oft unter Verletzung von Vorschriften,⁹³ die zur Geheimhaltung von diesen Daten verpflichten, verkauft oder weitergeleitet werden. Nicht zuletzt fördert der Missbrauch der neuen Medien⁹⁴ die unbefugte Offenbarung von persönlichen Geheimnissen, die Mitgliedern bestimmter Berufsgruppen, etwa Rechtsanwälten, Wirtschaftsprüfern oder Ärzten, im Zusammenhang mit der Ausübung dieses Berufs anvertraut werden. Solche Handlungen können unter § 203 StGB subsumiert werden.

Im Jahr 2009 ist die Zahl der Verstöße gegen Vorschriften, die dem Persönlichkeitsschutz bzw. dem Datenschutz dienen, um 350% gegenüber dem Jahr 2008 gestiegen. Immer wieder wurden sensible beziehungsweise private Daten von Bürgern oder Kunden ungesichert ins Internet gestellt, soziale Netzwerke ließen Zugriffe auf vertrauliche Mitgliederdaten zu, Finanzdienstleister gaben Tausende von Kundeninformationen unberechtigterweise weiter und Telekomprovider und Webshops schickten private Daten an fremde Personen. Auch öffentliche Stellen, wie etwa Stadtverwaltungen, Gerichte und die Bundesagentur für Arbeit, haben wiederholt die Datenschutzvorschriften verletzt. Denn nach wie vor sind keine Maßnahmen getroffen, die den Persönlichkeitsschutz effizient gewähren können.⁹⁵

Im April 2013 sollen Hacker in den Besitz persönlicher Daten wie Name, Mail-Adresse, Geburtsdatum und verschlüsseltes Passwort, die auf den Servern des Schnäppchenmarktes LivingSocial hinterlegt waren, gelangt sein. Die Betreiber des LivingSocial haben rund 50 Millionen ihrer Kunden aufgefordert, ein neues Passwort zu setzen. Die Datenbanken, in denen die Informationen zu den Kreditkarten der Anwender und die finanziellen Informationen zu den Händlern liegen, waren anscheinend nicht das Ziel des Angriffs.⁹⁶

Im Mai 2013 hat ein US-Bundesgericht in New York den sog. 28-jährigen "Stratfor-Hacker" zu einer Freiheitsstrafe von zehn Jahren verurteilt. Das Anonymous-Mitglied hatte die Datenbestände diverser Behörden und Unternehmen kopiert. Vom privaten Nachrichtendienst Strategic Forecasting, Inc, ("Stratfor") habe er mindestens 200 GByte heruntergeladen, die Daten von ungefähr 860.000 Kunden. Dazu gehörten Zehntausende von Kreditkartenkonten, mit deren Hilfe mindestens 700.000 US-Dollar an gemeinnützige Organisationen überwiesen worden seien. Der Täter hatte sich schuldig bekannt. Anderenfalls hätte ihm eine noch

⁹³ Etwa § 43 Abs. 1 Nr. 4 BDSG.

⁹⁴ Etwa die Manipulation von ärztlichen Datenbanken.

⁹⁵ <http://www.datenschutz-praxis.de/fachwissen/fachnews/datenschutz-verstose-rekordjahr-2009>.

⁹⁶ <http://allthingsd.com/20130426/livingsocial-hacked-more-than-50-million-customer-names-emails-birthdates-and-encrypted-passwords-accessed/>.

deutlich längere Haftstrafe gedroht. Die Richterin zeigte keinerlei Verständnis für die vom Täter vorgebrachten gesellschaftlichen und politischen Motive.⁹⁷

Persönliche Daten von mehr als 300.000 Studenten und Angestellten einer Universität im US-Bundesstaat Maryland haben Hacker erbeutet. Bei den gestohlenen Informationen handelt es sich unter anderem um Namen, Geburtsdaten und Sozialversicherungsnummern. Die Informationen von Studenten und Angestellten in der Datenbank reichten bis 1998 zurück. Es habe sich um einen äußerst ausgeklügelten Hacker-Angriff gehandelt, teilte die Universität mit.⁹⁸

Ende Januar 2015 haben Hacker die Datenbank der zweigrössten US-Krankenkasse attackiert und haben dabei die persönlichen Daten von Millionen Kunden erbeutet. Das Unternehmen teilte mit, die Täter haben sich Datensätze mit Namen, Geburtsdaten, Kranken- und Sozialversicherungsnummern, Postanschriften, E-Mail-Adressen, Anstellungsverhältnissen und Gehaltsauskünften aneignet. Es wurde allerdings nicht festgestellt, wie viele der ca. 68 Millionen Mitglieder betroffen waren.⁹⁹

Während eines Ermittlungsverfahrens hat die Staatsanwaltschaft Verden einen Datensatz mit 18 Millionen E-Mail-Adressen und den dazugehörigen Passwörtern erhalten. Betroffen sind neben ausländischen Firmen alle großen deutschen E-Mail-Provider. Manche der Zugangsdaten würden aktuell für Angriffe missbraucht. Es ist noch nicht bekannt, wie viele der Zugangsdaten deutschen Nutzern zuzurechnen ist. Die Behörden gehen von etwa drei Millionen betroffenen Bundesbürgern aus. Es handelt sich um den größten bisherigen Fall von Datendiebstahl in Deutschland.¹⁰⁰

Die sozialen Netzwerke haben auch neue Möglichkeiten gegeben, sich auf Opfer, insbesondere Kinder zu stürzen. Laut der BITKOM-Studie zur Nutzung sozialer Netzwerke in Deutschland waren 2013 zwei Drittel der deutschen Internetnutzer in sozialen Netzwerken aktiv.¹⁰¹ Durch das sog. Cybermobbing/Cyberbullying¹⁰² werden Menschen angepöbelt, angegriffen, schikaniert oder gequält, meist über einen längeren Zeitraum. Als Handlungen des Cybermobbing/Cyberbullying werden das Flaming (Beleidigung, Beschimpfung), Harassment (Belästigung), Denigration (Gerüchte verbreiten), Impersonation (Auftreten unter falscher Identität), Outing and Trickery (Bloßstellen und Betrügereien), Exclusion (Ausschluss), Cyberstalking

⁹⁷ <http://heise.de/-2047952>

⁹⁸ Dazu siehe Mitteilung der Universität vom 31.5.2014 <http://umd.edu/datasecurity/>

⁹⁹ <https://www.anthemfacts.com/>:

¹⁰⁰ Dazu siehe <http://www.spiegel.de/netzwelt/netzpolitik/e-mail-passwoerter-gestohlen-18-millionen-datensaetze-a-962419.html>

¹⁰¹ BITKOM-Studie 2013:
http://www.bitkom.org/files/documents/BITKOMPK_Studie_Nutzung_Sozialer_Netzwerke_31_10_2013.pdf.

¹⁰² Siehe Dazu LG Berlin Ur. V. 13.8.2012 – 33 O 434/11, ZUM 2012 S. 997, Glaser, NVwZ 2012, 1432.

(fortwährende Belästigung und Verfolgung), Cyberthreats (offene Androhung von Gewalt) genannt.¹⁰³

Mitte 2014 haben dutzende deutscher Blogger festgestellt, dass Unbekannte ihre Blogs eins zu eins spiegeln und veröffentlichen. Die Täter melden den Domain-Namen des Blogs in anderen Top-Level-Domain-Zonen an. Beispielsweise nutzen sie statt des echten Namens *einbeispielblog.de* die Alternativen *einbeispielblog.net* oder *einbeispielblog.com*, falls diese verfügbar sind. Offensichtlich verdienen die unbekanntenen Täter mit dem fremden Blog-Content. Wahrscheinlich versuchen sie mit den Blog-Spiegelungen Klicks auf Werbebanner von Affiliate-Netzwerken zu erzeugen. Dazu könnten sie sich beispielsweise der Cookie-Dropping-Technik bedienen, um Klicks auf Werbebanner ihren anonym angelegten Accounts bei Affiliate-Netzwerken zuordnen zu lassen.¹⁰⁴

Demnach stellen solche Missbrauchsfälle mediengenerierte Delikte dar, die sich gegen die Persönlichkeit im weiteren Sinne richten

Nach einer Studie der Universität Münster vom 2011 sind 32 % der Jugendlichen und jungen Erwachsenen als Opfer von Cybermobbing betroffen.¹⁰⁵ Die Folgen von Cybermobbing fallen unterschiedlich aus. Die Opfer berichten von emotionalen Folgen, sie fühlen sich wütend, verzweifelt, verletzt oder hilflos. Eine große Diskussion über das Cybermobbing wurde in der Bundesrepublik durch den Selbstmord der Schülerin „Megan Meier“ im Jahr 2006 ausgelöst.¹⁰⁶

Nach Angaben der Interpol sind Anfang Mai 2014 mit der Operation „Strikeback“ 58 Verdächtige festgenommen worden, die für von den Philippinen aus operierende Verbrecherbanden arbeiteten. Darunter waren auch drei Männer, die durch ihre Drohungen vermutlich einen Teenager aus Schottland in den Selbstmord getrieben haben. Betrüger verleiten ihre Opfer dazu, freizügige Bilder von sich preiszugeben, und erpressen sie dann damit. Der 17-Jährige hatte sich im vergangenen Jahr vor seiner Internetkamera ausgezogen, weil er glaubte, Kontakt mit einem Mädchen zu haben. Am anderen Ende der Leitung waren in Wirklichkeit allerdings Betrüger, die ihn anschließend mit dem Videomaterial erpressten. Der Teenager stürzte sich von einer Brücke. Diese Handlung wird als "Sextortion" bezeichnet (von engl. *extortion* für Erpressung). Nach Schätzung von Interpol sind weltweit bereits Hunderttausende Internetnutzer Opfer von ähnlichen Erpressungen geworden. Im Schnitt verlangten die Täter 500 Dollar von ihren Opfern. Auch Forderungen in Höhe von 15.000 Dollar habe es aber schon gegeben.¹⁰⁷

¹⁰³ IuK-Kriminalität in NRW, Lagebild 2011, S. 15.

¹⁰⁴ Siehe dazu <http://heise.de/-2297045>

¹⁰⁵ Porsch/Pieschl/Hohage, Cybermobbing, S. 10.

¹⁰⁶ Cyber-Mobbing, Tod Einer Schülerin, Spiegel Online, 2007.

¹⁰⁷ Siehe dazu <http://www.interpol.int/News-and-media/News/2014/N2014-075>